



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 4 月 1 6 日
Date of Application:

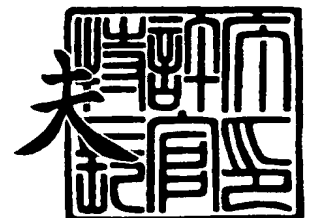
出 願 番 号 特 願 2 0 0 3 - 1 1 2 1 1 0
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 1 1 2 1 1 0]

出 願 人 日 本 電 気 株 式 会 社
Applicant(s):

2 0 0 4 年 1 月 2 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 53211064

【提出日】 平成15年 4月16日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14
H04B 7/26
H04M 1/675

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 塚本 直史

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100084250

【弁理士】

【氏名又は名称】 丸山 隆夫

【電話番号】 03-3590-8902

【手数料の表示】

【予納台帳番号】 007250

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9303564

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ユーザデータ保護方法、プログラムおよび携帯端末

【特許請求の範囲】

【請求項 1】 U I Mカードの使用によりユーザデータを本体から分離保有する携帯端末で用いられ、前記ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、

前記U I Mカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、

前記ユーザデータを前記識別情報毎に前記フォルダに分類するフォルダ分類ステップと、

前記識別情報を暗号鍵として用いて、前記ユーザデータを暗号化して保存する暗号化ステップと、

複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、

前記携帯端末内の前記ユーザデータを、前記U I Mカード内の識別情報と関連付けし、前記ユーザデータを保護することを特徴とするユーザデータ保護方法。

【請求項 2】 前記フォルダの作成は、前記携帯端末のユーザデータ保存領域に記録されることを特徴とする請求項 1 記載のユーザデータ保護方法。

【請求項 3】 前記フォルダは、前記U I Mカードの前記識別情報の数に応じて作成されることを特徴とする請求項 1 記載のユーザデータ保護方法。

【請求項 4】 前記動的管理は、前記ユーザデータを可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理することを特徴とする請求項 1 記載のユーザデータ保護方法。

【請求項 5】 前記静的管理は、不揮発性メモリ上に固定領域を確保し、前記ユーザデータのヘッダ部分にタグをつけて、利用可能なユーザを判断することを特徴とする請求項 1 記載のユーザデータ保護方法。

【請求項 6】 前記識別情報は、前記携帯端末が有する暗号処理ソフトウェアブロックによって暗号化処理され、暗号鍵となることを特徴とする請求項 1 記載のユーザデータ保護方法。

【請求項 7】 前記暗号処理ソフトウェアブロックは、前記 UIM カードの挿入の有無に関わらず、前記携帯端末の電源オン時に起動されることを特徴とする請求項 6 記載のユーザデータ保護方法。

【請求項 8】 前記暗号処理ソフトウェアブロックは、前記ユーザの操作によって、前記コンテンツが変更された場合、変更内容を暗号化した後で前記識別情報を暗号鍵として前記フォルダ内に保存することを特徴とする請求項 6 記載のユーザデータ保護方法。

【請求項 9】 前記暗号処理ソフトウェアブロックは、前記 UIM カードから読み出された前記識別情報を一時記憶することを特徴とする請求項 7 または 8 のいずれか 1 項に記載のユーザデータ保護方法。

【請求項 10】 前記暗号処理ソフトウェアブロックは、前記一時記憶した個人識別情報を用いて、前記携帯端末内のコンテンツの暗号化および暗号解読処理を行うことを特徴とする請求項 9 記載のユーザデータ保護方法。

【請求項 11】 前記識別情報は、IMS I および ICC シリアルの内いずれか一方であることを特徴とする請求項 1 から 10 のいずれか 1 項に記載のユーザデータ保護方法。

【請求項 12】 前記フォルダは前記ユーザ操作によって作成されることを特徴とする請求項 1 記載のユーザデータ保護方法。

【請求項 13】 UIM カードの使用によりユーザデータを本体から分離保有する携帯端末のユーザデータ保護方法をコンピュータに実行させるプログラムであって、

前記 UIM カードの識別情報に関連付けられたフォルダを作成するフォルダ作成処理と、

前記ユーザデータを前記識別情報毎に前記フォルダに分類するフォルダ分類処理と、

前記識別情報を暗号鍵として用いて、前記ユーザデータを暗号化して保存する暗号化処理と、

複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成処理と、

をコンピュータに実行させることを特徴とするプログラム。

【請求項 1 4】 請求項 1 から 1 2 のいずれか 1 項に記載のユーザデータ保護方法を実施することを特徴とする携帯端末。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、U I Mカード等を用いて加入者情報と端末本体を分離保有可能な携帯端末に用いられるユーザデータ保護方法、プログラムおよび携帯端末に関する。

【0 0 0 2】

【従来技術】

第三世代携帯電話機においては、加入者情報と携帯電話機本体が分離しており、ユーザは自身の加入者情報が記録されたU I Mカードを保有し、任意の携帯電話機に挿入してサービスを利用することが可能である。個人のプライバシーはU I Mカードに由来しており、契約情報も含めた重要な個人データは全てU I Mカード内に保持されることが理想である。

【0 0 0 3】

しかしながら、U I Mカードのサイズ／容量上の制限により、U I Mカードに全てユーザデータを保持することは不可能であり、メールや電話帳、アプリケーションなど、ユーザ個人が利用するコンテンツの殆どは携帯電話機本体に記録されることになる。

【0 0 0 4】

従って、ある個人の携帯電話機に他人のU I Mカードが挿入された場合、そのU I Mカードの契約情報に基づいたサービスを利用できると同時に、内部のコンテンツは他人によって自由に使用並びに変更ができることになる。例としては、①発着信履歴が残る。②挿入された他人のU I Mカードに宛てられたメール等が記録される。③NW利用型コンテンツの使用が可能となる（NW接続を利用するアプリケーション等）。④内蔵コンテンツの追加および削除、といった操作が可能となる。

【0005】

また、UIMカードを挿入せずに携帯電話機の電源を投入した場合、携帯電話のサービスを利用することは不可能であるが、内部のコンテンツは自由に使用できる。

【0006】

以上のことから、従来の日本国内における携帯電話機（第三世代以前）では、携帯電話機自体の不揮発領域に個人契約情報が記録されているため、「個人情報の管理＝携帯電話機内のコンテンツの管理」という図式が成立するが、第三世代においては前述の通り、契約情報を含めた個人データはUIMカードに由来するため、1台の携帯電話機を複数の契約者で共有する機会が格段に増すことから、第3世代携帯における個人データを保護が必要となる。

【0007】

従来の技術例として、ユーザデータを不揮発性メモリへ格納する構成の携帯端末において、ユーザデータの書き込み時の消失や不正化を防止する「携帯端末とそのユーザデータ保護方法」がある（例えば、特許文献1参照）。また、ユーザの識別情報やユーザが独自に決めた識別情報を、キーワードを用いて自動的に暗号化および解読する「情報の暗号化／解読方法と同システム」がある（例えば、特許文献2参照）。また、SIMカードを用いて利用した携帯電話機を他者に渡した場合、内部に記録されたプライベートな個人データの閲覧を防止できる「加入者カードを用いる携帯電話機」がある（例えば、特許文献3参照）。

【0008】**【特許文献1】**

特開 2001-101079号公報

【特許文献2】

特開 2002-281022号公報

【特許文献3】

特開 2002-300254号公報

【0009】

【発明が解決しようとする課題】

上記特許文献1記載の発明は、UIMカード等を使用する第3世代携帯端末に対応していない構成である。また、特許文献2記載の発明は、データの暗号化に用いるキーワードがユーザによって作成されるものであり、UIMカード内の識別情報を用いるものではなく、第3世代携帯端末に対応していない構成である。また、特許文献3記載の発明は、第3世代携帯に対応する構成ではあるが、データ保護のために外付けのメモリを必要とする。

【0010】

よって、外付けの装置を必要とせず、第3世代携帯端末の構成に対応可能であり、UIMカードなしで端末の電源を入れた際に、内部のユーザデータの閲覧を不可能とするユーザデータ保護方法が望まれる。

【0011】

本発明は、上記事情に鑑みてなされたものであり、UIMカード等により加入者情報と本体を分離保有可能な携帯端末において、携帯端末内のユーザデータをUIMカード内の識別情報と関連付けし、個人の固有データを保護するユーザデータ保護方法、プログラムおよび携帯端末を提供することを目的とする。

【0012】

また、本発明は、携帯電話機が複数の契約者によって共有利用されることを前提とし、本体に記録されるコンテンツのプライバシー保護について、UIMカード内の識別情報(IMS I)を関連させ、他人のUIMカードが挿入された場合にも、暗号鍵となるUIMカードの識別情報が異なるため、他人内部のユーザデータの閲覧が不可能となるユーザデータ保護方法、プログラムおよび携帯端末を提供することを目的とする。

【0013】

【課題を解決するための手段】

かかる目的を達成するために、請求項1記載のユーザデータ保護方法は、UIMカードの使用によりユーザデータを本体から分離保有する携帯端末で用いられ、ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、UIMカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、ユーザデータを識別情報毎にフォルダに分類する

フォルダ分類ステップと、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化ステップと、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、携帯端末内のユーザデータを、UIMカード内の識別情報と関連付けし、ユーザデータを保護することを特徴とする。

【0014】

請求項2記載のユーザデータ保護方法は、請求項1記載のユーザデータ保護方法において、フォルダの作成は、携帯端末のユーザデータ保存領域に記録されることを特徴とする。

【0015】

請求項3記載のユーザデータ保護方法は、請求項1記載のユーザデータ保護方法において、フォルダは、UIMカードの前記識別情報の数に応じて作成されることを特徴とする。

【0016】

請求項4記載のユーザデータ保護方法は、請求項1記載のユーザデータ保護方法において、動的管理は、ユーザデータを可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理することを特徴とする。

【0017】

請求項5記載のユーザデータ保護方法は、請求項1記載のユーザデータ保護方法において、静的管理は、不揮発性メモリ上に固定領域を確保し、ユーザデータのヘッダ部分にタグをつけて、利用可能なユーザを判断することを特徴とする。

【0018】

請求項6記載のユーザデータ保護方法は、請求項1記載のユーザデータ保護方法において、識別情報は、携帯端末が有する暗号処理ソフトウェアブロックによって暗号化処理され、暗号鍵となることを特徴とする。

【0019】

請求項7記載のユーザデータ保護方法は、請求項6記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、UIMカードの挿入の有無に関わらず、携帯端末の電源オン時に起動されることを特徴とする。

【 0 0 2 0 】

請求項 8 記載のユーザデータ保護方法は、請求項 6 記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ユーザの操作によって、コンテンツが変更された場合、変更内容を暗号化した後で識別情報を暗号鍵としてフォルダ内に保存することを特徴とする。

【 0 0 2 1 】

請求項 9 記載のユーザデータ保護方法は、請求項 7 または 8 のいずれか 1 項に記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、U I Mカードから読み出された識別情報を一時記憶することを特徴とする。

【 0 0 2 2 】

請求項 1 0 記載のユーザデータ保護方法は、請求項 9 記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、一時記憶した個人識別情報を用いて、携帯端末内のコンテンツの暗号化および暗号解読処理を行うことを特徴とする。

【 0 0 2 3 】

請求項 1 1 記載のユーザデータ保護方法は、請求項 1 から 1 0 のいずれか 1 項に記載のユーザデータ保護方法において、識別情報は、I M S I および I C C シリアル のいずれか一方であることを特徴とする。

【 0 0 2 4 】

請求項 1 2 記載のユーザデータ保護方法は、請求項 1 記載のユーザデータ保護方法において、フォルダはユーザ操作によって作成されることを特徴とする。

【 0 0 2 5 】

請求項 1 3 記載のプログラムは、U I Mカードの使用によりユーザデータを本体から分離保有する携帯端末のユーザデータ保護方法をコンピュータに実行させるプログラムであって、U I Mカードの識別情報に関連付けられたフォルダを作成するフォルダ作成処理と、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類処理と、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化処理と、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成処理とをコンピュータに

実行させることを特徴とする。

【 0 0 2 6 】

請求項 1 4 記載の携帯端末は、請求項 1 から 1 2 のいずれか 1 項に記載のユーザデータ保護方法を実施することを特徴とする。

【 0 0 2 7 】

【発明の実施の形態】

以下、本発明の実施形態について、添付図面を参照しながら詳細に説明する。

【 0 0 2 8 】

U I Mカード等により加入者情報と本体を分離保有可能な携帯電話機の一般的な装置構成を図 2 に示す。U I Mカード 8 には I M S I (International Mobile Station Identifier) と呼ばれる、加入者情報を識別するための唯一無二の情報要素が内包されている。利用者はこの U I Mカード 8 を携帯電話機本体に装着することにより、携帯電話網への接続し、契約するサービスを利用することができる。携帯電話機本体はユーザデータを永続的に保存するための不揮発性メモリ 1 1 (あるいは常時バックアップされる揮発性メモリ) を有している。

【 0 0 2 9 】

ユーザデータとは電話帳、メール、発着信履歴、その他のコンテンツ、更には携帯電話機操作部のカスタマイズ情報 (例えば、画面上に置かれたアイコンの配置情報) などとも指し示す。

【 0 0 3 0 】

図 3 に示すように、ユーザデータの保存方法としては、1 つ 1 つのコンテンツを各々固定サイズのエリアに格納する方式 (静的管理方式) や、可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理する方式 (動的管理方式) などがある。これらのユーザデータは、装置電源 O N 時、あるいはユーザ操作によりデータ読出し時に、不揮発性メモリ領域から一旦一時メモリ領域に展開されて利用される。ユーザデータの変更等は、まず一時メモリ領域に展開されたデータを変更し、不揮発メモリ領域に反映される。不揮発メモリ領域を書き換えるタイミングは、コンテンツ毎の性質により異なる。

【 0 0 3 1 】

次に本発明における、ユーザデータの保護方法のイメージを図1に示す。本発明において、携帯電話機内のユーザデータは動的管理されることを前提とする。携帯電話機のユーザデータ保存領域には、IMS Iに関連付けられた「フォルダ」情報が記録され、個人のユーザデータは契約しているUIMカードのIMS Iに従って、フォルダ分けされる。このフォルダ情報は携帯電話機を共有使用するUIMカードのIMS Iの数だけ作成される。必要に応じてユーザ操作により、新たなフォルダを作成することも可能とする。また、共通に利用できるコンテンツを保存する機能を有するため、「共有フォルダ」が作成される。

【0032】

さらに、携帯電話機は、図2の中央制御部内にUIM内のIMS Iを用いた暗号化／解読処理を実施する暗号処理ソフトウェアブロック13を有している。この暗号処理ソフトウェアブロック13の機能は大きく以下の通りである。

(1) UIMカードより読み出されたIMS I情報を一時記憶する機能（他のソフトウェアブロックと共通でありうる）。

(2) 一時記憶されたIMS Iを用いて、携帯電話機内のコンテンツを暗号化／暗号解読処理を実施する機能。

【0033】

携帯電話機のメインプログラムは、装置電源ON時にUIMカードが挿入有無に関わらず、必ずこの暗号処理ブロックを起動する。また、携帯電話機操作にて内蔵するコンテンツ情報が変更された場合は、必ずこの暗号処理ソフトウェアブロック13を起動し、IMS Iを暗号鍵として変更内容を暗号化した後で、IMS Iに関連されたフォルダ内に保存する。

【0034】

例えば、図4において、IMS I = [B] というUIMカードが使用されている場合は、IMS Iに関連付けられたフォルダ内のファイルと、共有フォルダ内のファイルのみが移動機本体にて使用可能となる。

【0035】

次に、図5から図7を参照して本発明の実施形態の動作を説明する。

【0036】

装置電源投入時の動作について図5を参照して説明する。中央制御部に電源供給開始し、装置の初期設定を行う（S501）。UIMカードが装置に挿入されているかを調べる（S502）。挿入されていない場合は（S502/NO）、暗号処理ブロックを起動する（S506）。挿入されている場合（S502/YES）、本体に挿入されたUIMカードを活性化し（S503）、さまざまな情報を読み出す（S504）。UIMカードより読み出したIMSIを一時記憶する（S505）。暗号処理ブロックを起動する（S506）。メインプログラムが「共有フォルダ」内の情報を読み出す（S507）。このフォルダ内の情報は暗号解読を行わない。メインプログラムが一時記憶されたIMSIが存在し（S508/YES）、IMSIに関連付けられたフォルダ（IMSI固有フォルダ）がある場合（S509/YES）、一時記憶IMSIを参照し、IMSI固有フォルダ内の情報を読み出す（S510）。暗号処理ブロックが一時記憶されたIMSIを暗号鍵として、ユーザデータ保存領域のデータを読み出し、解読する（S511）。共有データと解読されたユーザデータを、一時メモリ領域に展開する（S512）。一時記憶IMSI、IMSI固有フォルダのどちらかがない場合は（S508/NO、S509/NO）、読み出しおよび処理を行わず、そのまま共有データと解読されたユーザデータを、一時メモリ領域に展開する（S512）。

【0037】

装置操作によるユーザデータ読み出し時の動作について図6を参照して説明する。指定したユーザデータが共有データの場合（S601/YES）、「共有フォルダ」より情報を読み出し（S603）、暗号解読せずに指定データを展開する（S609）。指定したユーザデータがIMSIに関連付けられた暗号化データの場合（S602/NO、S604/YES、S605/YES）、暗号化ブロックを起動する（S606）。IMSIに関連づけられたフォルダより情報を読み出す（S607）。記憶したIMSIを用いて暗号を解読する（S608）。指定データを展開する（S609）。

【0038】

装置操作によるユーザデータ保存時の動作について図7を参照して説明する。

電話帳入力やメール送受信、NWからのダウンロード等によって得られたコンテンツが一時的メモリ領域に記録される。得られたコンテンツの保存操作を実行する。このとき、共有データとして保存するか、暗号化して保存するかを選択をユーザ操作により指定できることとする（S701）。指定したユーザデータが共有データの場合（S702/YES）、「共有フォルダ」内に暗号化無しで保存する（S703）。

【0039】

指定したユーザデータがIMSIに関連付けられた暗号化データの場合（S702/NO、S704/YES、S705/YES）、暗号化ブロックを起動する（S706）。暗号解読処理後（S707）、一時メモリ領域上のユーザデータに対して、IMSIを暗号鍵とした暗号化処理を実施し（S708）、指定の不揮発保存領域に記憶する。S705においてIMSI固有フォルダがない場合（S705/NO）、IMSI固有フォルダを作成するかを選択し（S709）、フォルダ作成後（S710）、暗号処理ブロックを起動し（S706）、同様の処理を行う。

【0040】

以上、本発明の実施形態によれば、第1の効果として、UIMカードにより加入者情報と本体を分離保有可能な携帯電話機において、携帯電話機内のユーザデータをUIMカード内の識別情報と関連付けし、個人の固有データを保護できる。第2の効果として、上記識別情報に関連した個人の固有データを、同じく識別情報に基づいて暗号化することにより、個人の固有データ保護を強固にできる。

【0041】

また、他の実施形態1として、暗号化処理とフォルダ分けをIMSIではなく、同じくUIMカードの固有情報である「ICCシリアル」によって行うことも可能である。また、他の実施形態2として、静的管理において、本発明の概念を適用した場合、不揮発性メモリ上に固定領域を確保する。複数ユーザでシェアする場合、ユーザごとに固定エリアを割当ててことは無駄が多いため、固有のユーザデータのヘッダ部分にタグをつけて、どのユーザによって利用可能かを判断する手段がある。

【 0 0 4 2 】**【発明の効果】**

以上の説明から明らかなように、請求項 1 記載のユーザデータ保護方法によれば、U I Mカードの使用によりユーザデータを本体から分離保有する携帯端末で用いられ、ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、U I Mカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類ステップと、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化ステップと、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、携帯端末内のユーザデータを、U I Mカード内の識別情報と関連付けし、ユーザデータを保護することを特徴とするので、U I Mカードなしで携帯電話機の電源を投入した際、内部のユーザデータの閲覧を不可能とし、また、他人のU I Mカードが挿入された場合でも、暗号鍵となるU I Mカードの識別情報が異なるため、他人の内部ユーザデータ閲覧が不可能となる。

【 0 0 4 3 】

請求項 2 記載のユーザデータ保護方法によれば、請求項 1 記載のユーザデータ保護方法において、フォルダの作成は、携帯端末のユーザデータ保存領域に記録されることを特徴とするので、携帯電話機内のユーザデータをU I Mカード内の識別情報と関連付けし、個人の固有データを保護できる。

【 0 0 4 4 】

請求項 3 記載のユーザデータ保護方法によれば、請求項 1 記載のユーザデータ保護方法において、フォルダは、U I Mカードの前記識別情報の数に応じて作成されることを特徴とするので、携帯電話機内のユーザデータをU I Mカード内の識別情報と関連付けし、個人の固有データを保護できる。

【 0 0 4 5 】

請求項 4 記載のユーザデータ保護方法によれば、請求項 1 記載のユーザデータ保護方法において、動的管理は、ユーザデータを可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理することを特徴とするので、携帯電話

機内のユーザデータを U I Mカード内の識別情報と関連付けし、個人の固有データを保護できる。

【 0 0 4 6 】

請求項 5 記載のユーザデータ保護方法によれば、請求項 1 記載のユーザデータ保護方法において、静的管理は、不揮発性メモリ上に固定領域を確保し、ユーザデータのヘッダ部分にタグをつけて、利用可能なユーザを判断することを特徴とするので、携帯電話機内のユーザデータを U I Mカード内の識別情報と関連付けし、個人の固有データを保護できる。

【 0 0 4 7 】

請求項 6 記載のユーザデータ保護方法によれば、請求項 1 記載のユーザデータ保護方法において、識別情報は、携帯端末が有する暗号処理ソフトウェアブロックによって暗号化処理され、暗号鍵となることを特徴とするので、個人の固有データ保護を強固にする。

【 0 0 4 8 】

請求項 7 記載のユーザデータ保護方法によれば、請求項 6 記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、U I Mカードの挿入の有無に関わらず、携帯端末の電源オン時に起動されることを特徴とするので、個人の固有データ保護を強固にする。

【 0 0 4 9 】

請求項 8 記載のユーザデータ保護方法によれば、請求項 6 記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ユーザの操作によって、コンテンツが変更された場合、変更内容を暗号化した後で識別情報を暗号鍵としてフォルダ内に保存することを特徴とするので、個人の固有データ保護を強固にする。

【 0 0 5 0 】

請求項 9 記載のユーザデータ保護方法によれば、請求項 7 または 8 のいずれか 1 項に記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、U I Mカードから読み出された識別情報を一時記憶することを特徴とするので、個人の固有データ保護を強固にする。

【 0 0 5 1 】

請求項 1 0 記載のユーザデータ保護方法によれば、請求項 9 記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、一時記憶した個人識別情報を用いて、携帯端末内のコンテンツの暗号化および暗号解読処理を行うことを特徴とするので、個人の固有データ保護を強固にする。

【 0 0 5 2 】

請求項 1 1 記載のユーザデータ保護方法によれば、請求項 1 から 1 0 のいずれか 1 項に記載のユーザデータ保護方法において、識別情報は、IMS I および ICC シリアルの内いずれか一方であることを特徴とするので、どちらの識別情報でも暗号化ができ、個人の固有データ保護を強固にする。

【 0 0 5 3 】

請求項 1 2 記載のユーザデータ保護方法によれば、請求項 1 記載のユーザデータ保護方法において、フォルダはユーザ操作によって作成されることを特徴とするので、携帯電話機内のユーザデータを UIM カード内の識別情報と関連付けし、個人の固有データを保護できる。

【 0 0 5 4 】

請求項 1 3 記載のプログラムによれば、UIM カードの使用によりユーザデータを本体から分離保有する携帯端末のユーザデータ保護方法をコンピュータに実行させるプログラムであって、UIM カードの識別情報に関連付けられたフォルダを作成するフォルダ作成処理と、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類処理と、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化処理と、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成処理とをコンピュータに実行させることを特徴とするので、UIM カードなしで携帯電話機の電源を投入した際、内部のユーザデータの閲覧を不可能とし、また、他人の UIM カードが挿入された場合でも、暗号鍵となる UIM カードの識別情報が異なるため、他人の内部ユーザデータ閲覧が不可能となる。

【 0 0 5 5 】

請求項 1 4 記載の携帯端末によれば、請求項 1 から 1 2 のいずれか 1 項に記載

のユーザデータ保護方法を実施することを特徴とするので、U I Mカードなしで携帯電話機の電源を投入した際、内部のユーザデータの閲覧を不可能とし、また、他人のU I Mカードが挿入された場合でも、暗号鍵となるU I Mカードの識別情報が異なるため、他人の内部ユーザデータ閲覧が不可能となる。

【図面の簡単な説明】

【図 1】

本発明のユーザデータ保護方法を示すイメージ図である。

【図 2】

本発明の実施形態である携帯電話の構成を示すブロック図である。

【図 3】

従来のユーザデータ管理方法を示すイメージ図である。

【図 4】

本発明のU I Mカードが挿入された場合の使用可能なデータの一例を示すイメージ図である。

【図 5】

本発明の実施形態にかかる装置電源投入時の処理動作を示すフロー図である。

【図 6】

本発明の実施形態にかかるユーザデータ読み出し時の処理動作を示すフロー図である。

【図 7】

本発明の実施形態にかかるユーザデータ保存時の処理動作を示すフロー図である。

【符号の説明】

- 1 無線部
- 2 通信処理部
- 3 中央制御部
- 4 周辺制御部
- 5 電源制御部
- 6 共通バス

7 U I Mカード制御部

8 U I Mカード

9 レシーバ

1 0 マイク

1 1 不揮発メモリ

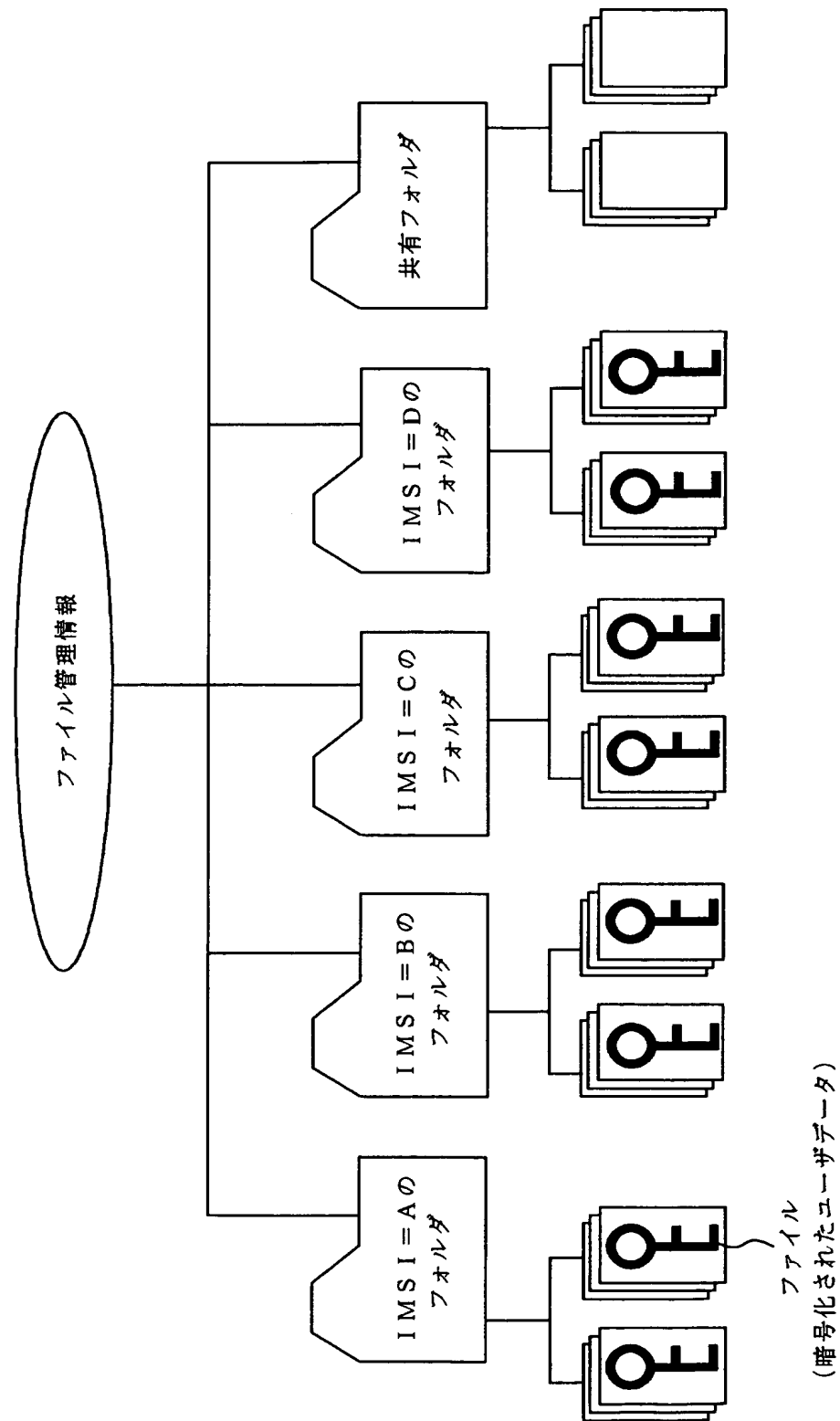
1 2 一時記憶用メモリ

1 3 暗号処理ソフト

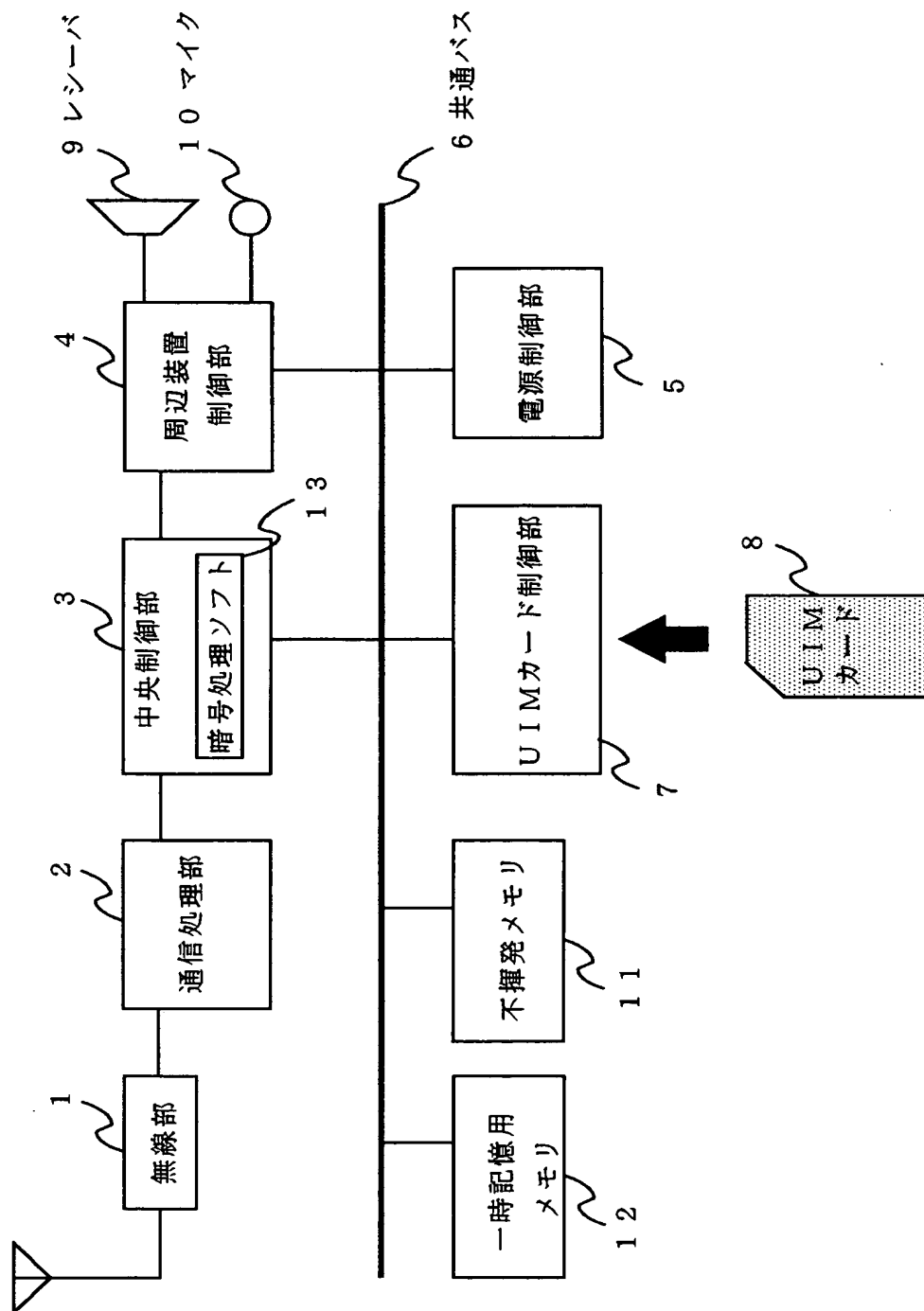
【書類名】

図面

【図 1】

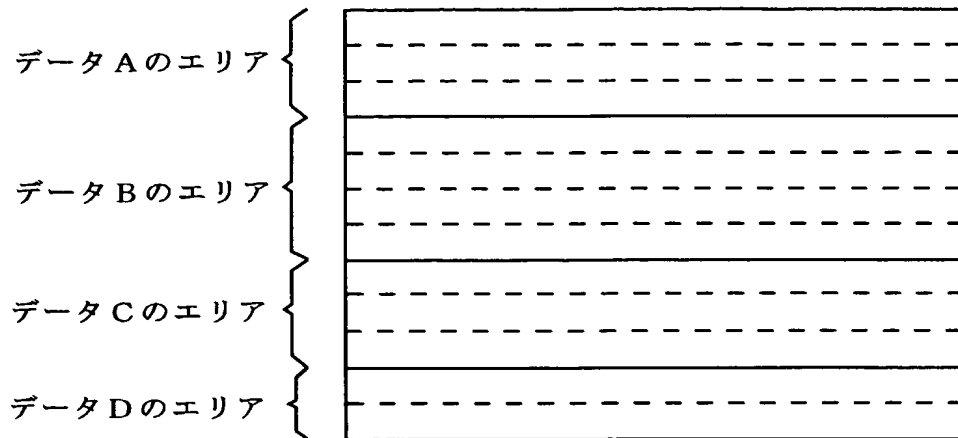


【図 2】

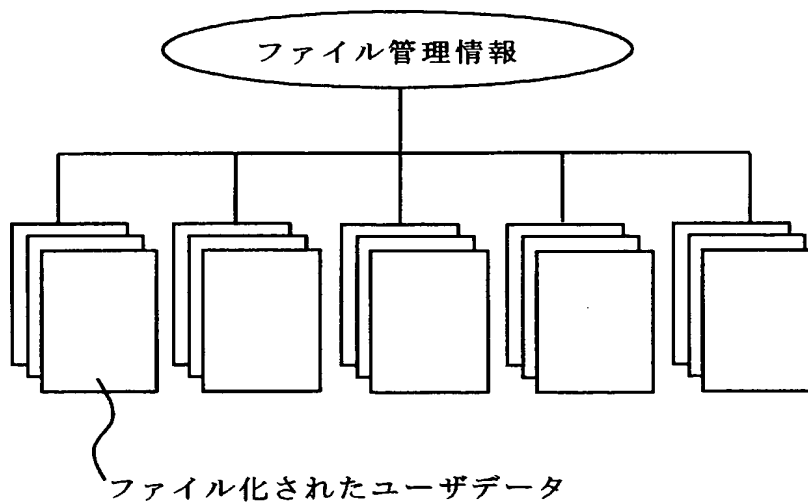


【図 3】

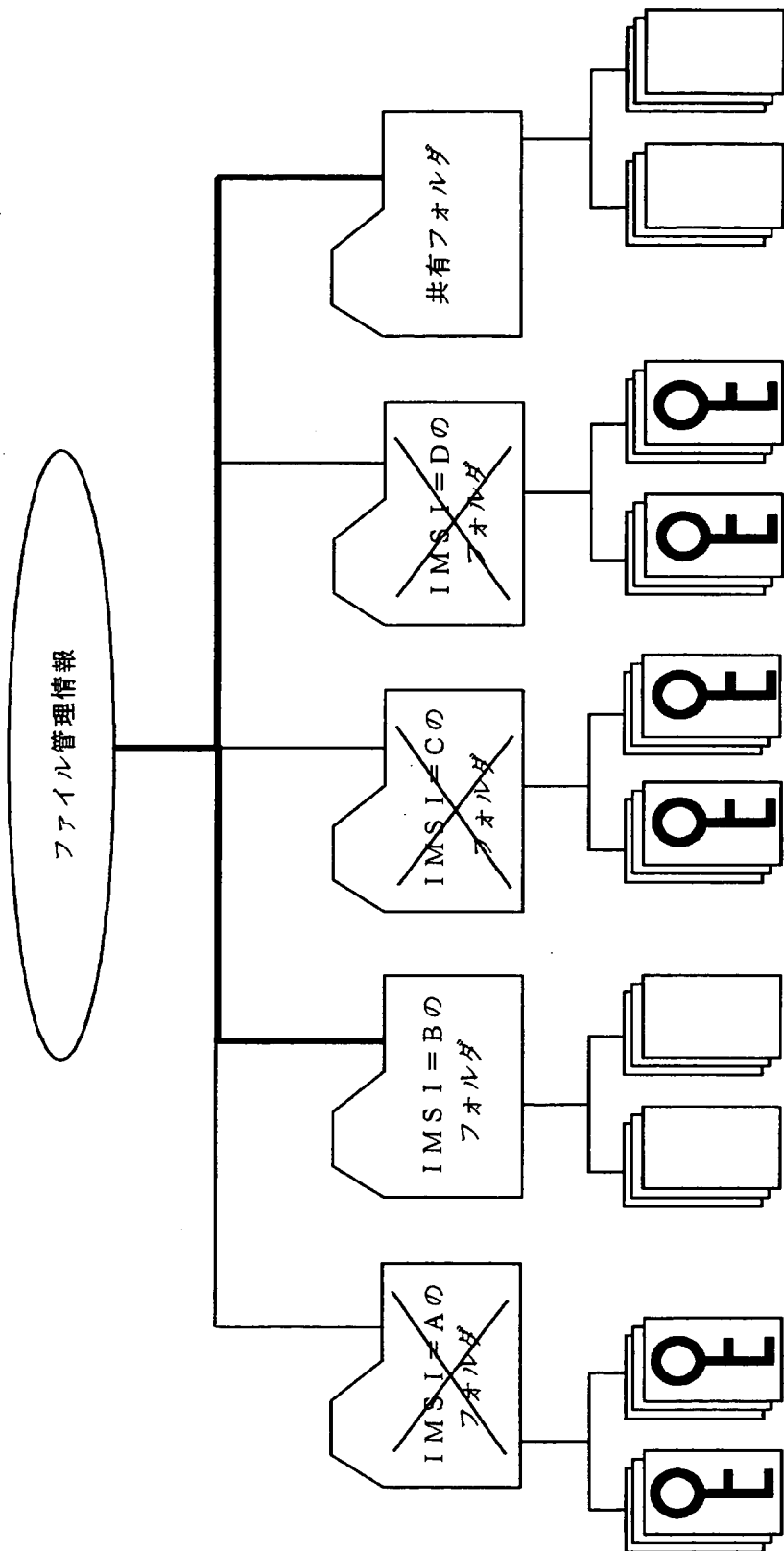
(a) ユーザデータを静的管理する場合



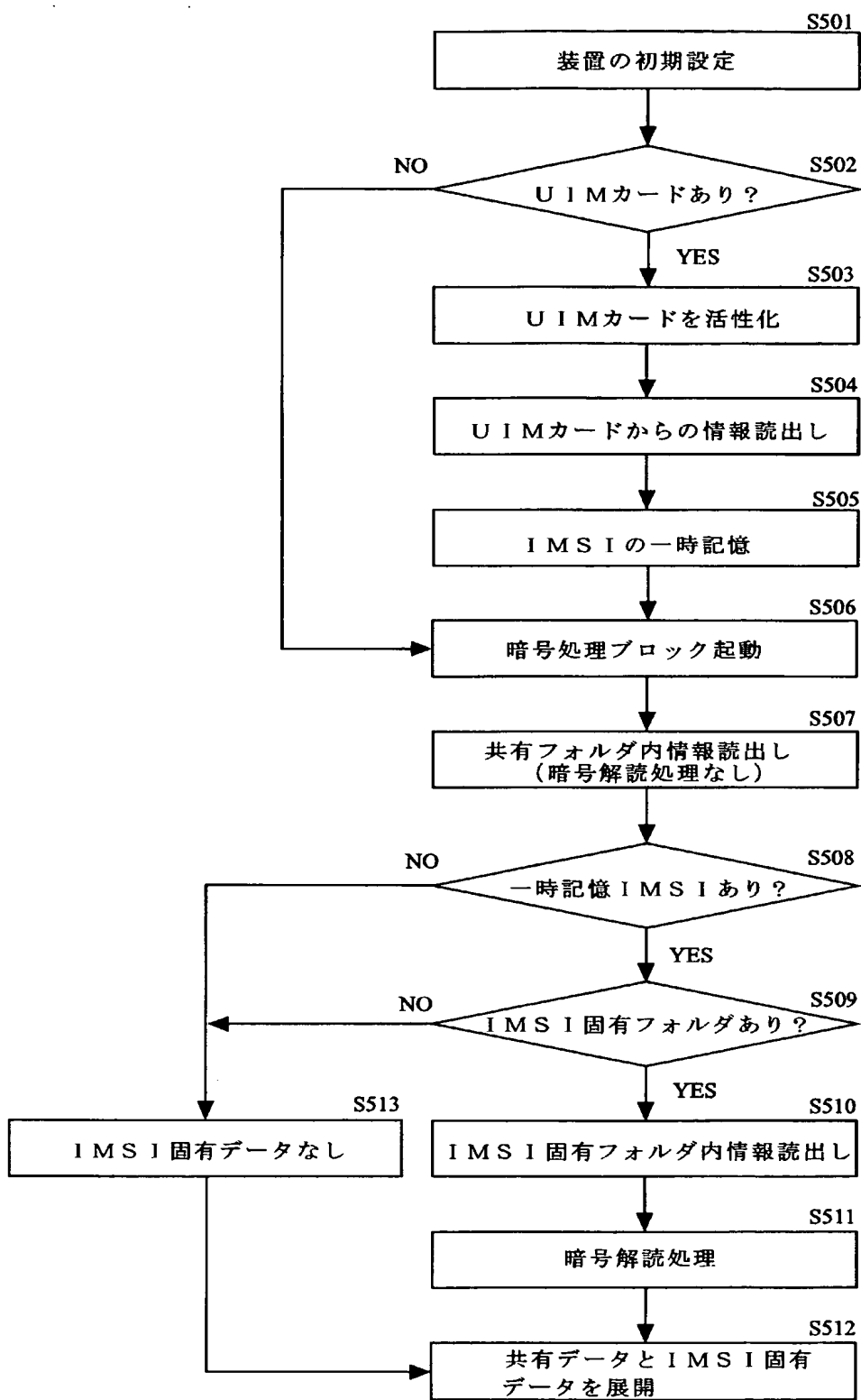
(b) ユーザデータを静的管理する場合



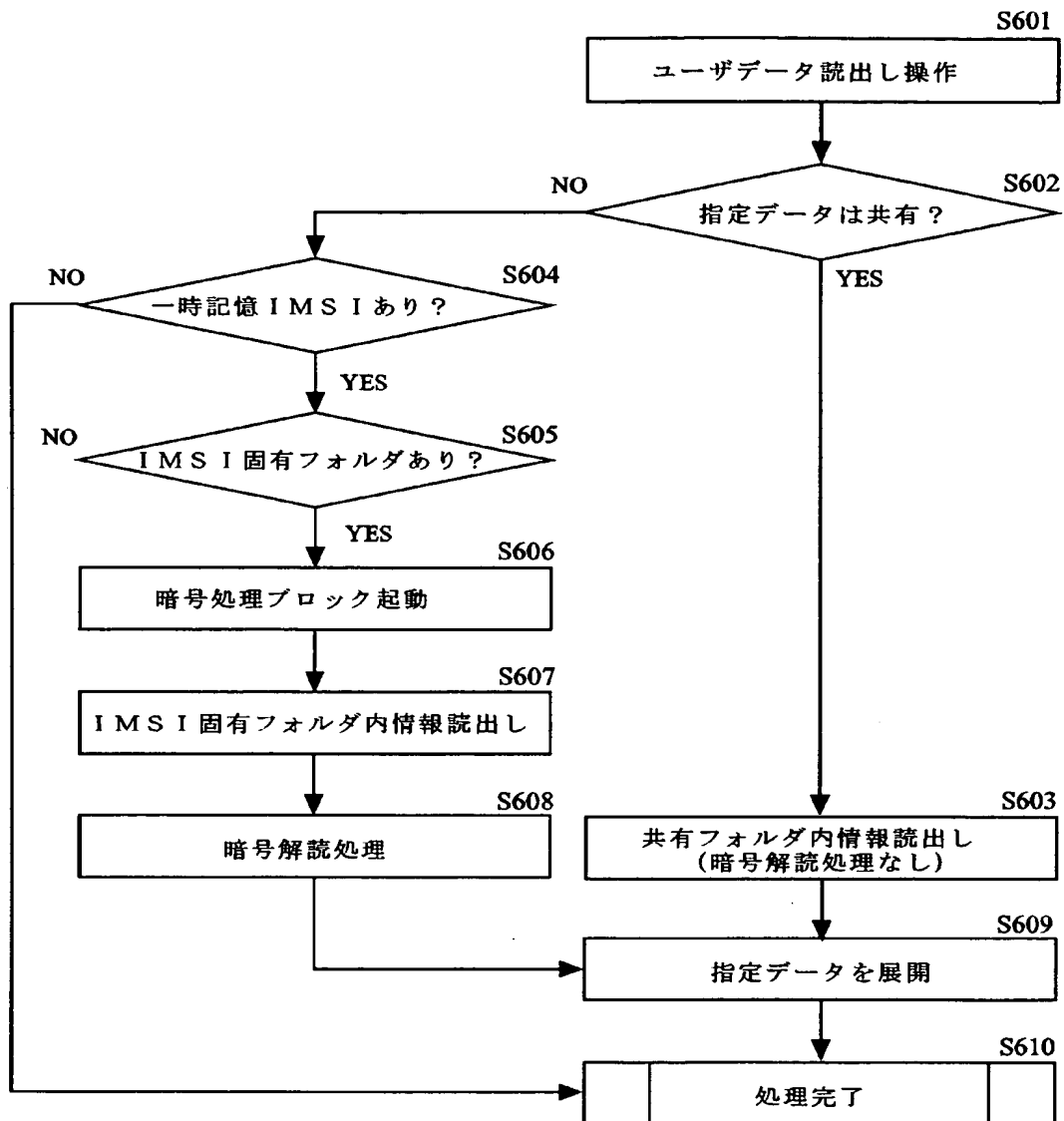
【図 4】



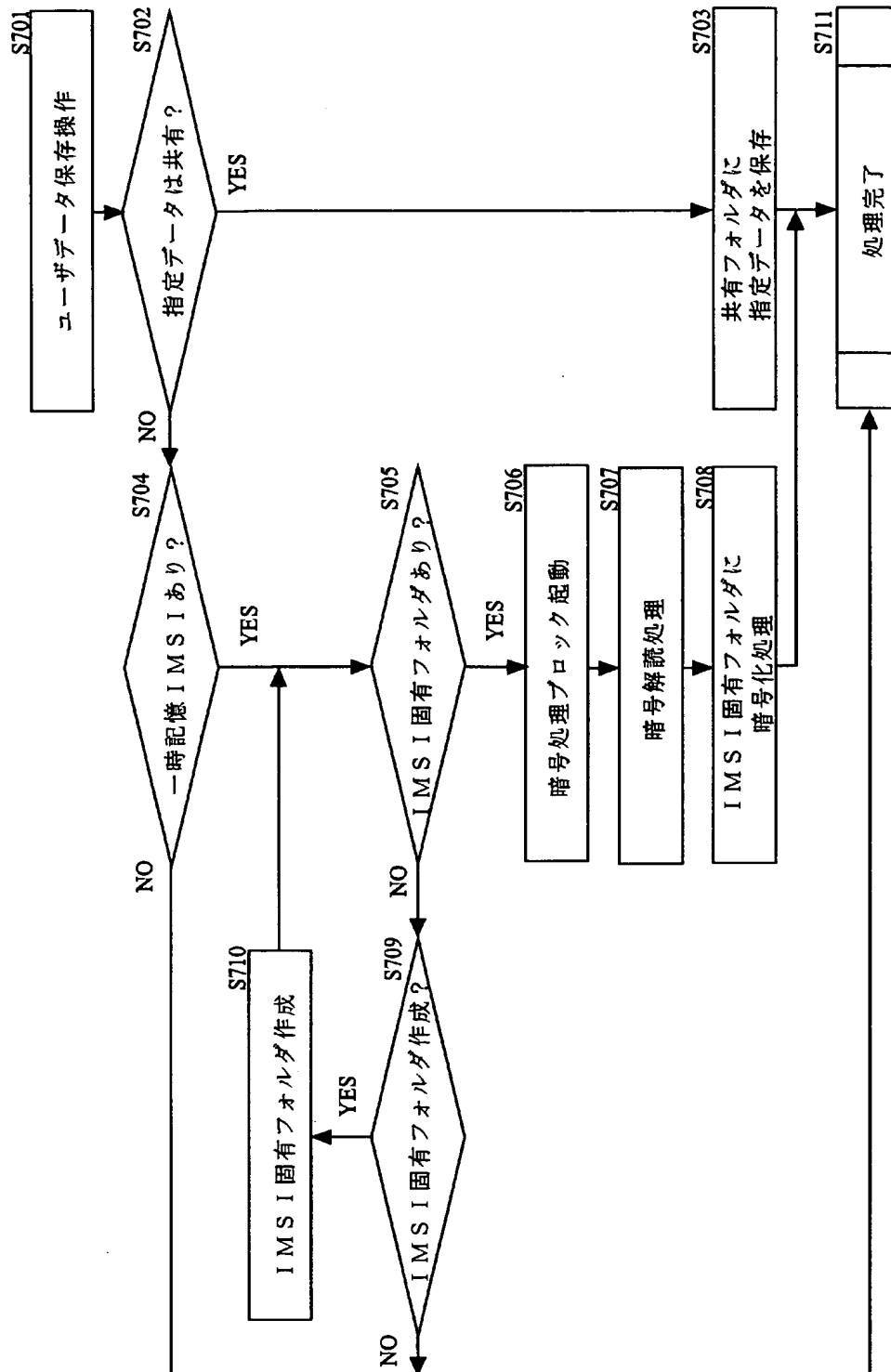
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 携帯端末内のユーザデータを U I Mカード内の識別情報と関連付けし、個人の固有データを保護するユーザデータ保護方法、プログラムおよび携帯端末を提供する。

【解決手段】 ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、U I Mカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類ステップと、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化ステップと、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、携帯端末内のユーザデータを U I Mカード内の識別情報と関連付けし、ユーザデータを保護する。

【選択図】 図 1

特願 2 0 0 3 - 1 1 2 1 1 0

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 2 3 7]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[変更理由]	新規登録
住 所	東京都港区芝五丁目 7 番 1 号
氏 名	日本電気株式会社